International Journal of Mathematical Education in Science and Technology

ISSN: 0020-739X (Print) 1464-5211 (Online) Journal homepage: https://www.tandfonline.com/loi/tmes20

General remainder theorem and factor theorem for polynomials over non-commutative coefficient rings

A. Cuida, F. Laudano & E. Martinez-Moro

To cite this article: A. Cuida, F. Laudano & E. Martinez-Moro (2019): General remainder theorem and factor theorem for polynomials over non-commutative coefficient rings, International Journal of Mathematical Education in Science and Technology, DOI: 10.1080/0020739X.2019.1676926

To link to this article: https://doi.org/10.1080/0020739X.2019.1676926

Published online: 20 Oct 2019.

Submit your article to this journal

Article views: 15

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=tmes20

INTERNATIONAL JOURNAL OF MATHEMATICAL EDUCATION IN SCIENCE AND TECHNOLOGY
https://doi.org/10.1080/0020739X.2019.1676926

NOTE

General remainder theorem and factor theorem for polynomials over non-commutative coefficient rings

A. Cuida [a], F. Laudano [b] and E. Martinez-Moro [c]

[a]GIR EduMat, Universidad de Valladolid, Valladolid, Spain; [b]Departement of Mathematics, University of Salerno, Fisciano (SA), Italy; [c]Institute of Mathematics, Universidad de Valladolid, Valladolid, Spain

ABSTRACT
We propose some generalizations of the classical Division Algorithm for polynomials over coefficient rings (possibly non-commutative). These results provide a generalization of the Remainder Theorem that allows calculating the remainder without using the long division method, even if the divisor has degree greater than one. As a consequence we obtain an extension of the classical Factor Theorem that provides a general divisibility criterion for polynomials. Finally, we will refer to some applications of these results for evaluating and dividing on skew polynomial rings. The arguments can be used in basic algebra courses and are suitable for building classroom/homework activities.

ARTICLE HISTORY
Received 24 April 2019

KEYWORDS
Remainder theorem; factor theorem; long division; left modulo-*m* congruence; polynomial divisibility criterion; non-commutative coefficient ring

2010 MATHEMATICS SUBJECT CLASSIFICATIONS
Primary: 13B25; Secondary: 11C08

1. Introduction

The classical Remainder Theorem and the Factor Theorem are typically studied in high school for polynomials with coefficients in the field $\mathbb{R}$ of real numbers (cf. McAskill et al., 2012, pp. 123 and 127 or Blitzer, 2014, p. 341). In this version, it states that the remainder of a polynomial $f \in \mathbb{R}[x]$ on division by a binomial $x - c \in \mathbb{R}[x]$ is $f(c)$; and that $x-c$ divides f in $\mathbb{R}[x]$ if and only if $f(c) = 0$.

This relation between evaluation and division is common folklore in algebra courses and goes back to the works of Horner and Ruffini. Horner's Method is named after an English school teacher and mathematician, William George Horner (1786–1837), who published a numerical method in 1819 to find approximate solutions to polynomial equations with coefficients in $\mathbb{R}$ (Joseph, 2011). Unlike other computational methods to find roots, Horner's method is more efficient because it requires fewer iterations to get the same result. Paolo Ruffini (1765–1822) discovered the method independently and used it to make polynomial division more efficient (Cajori, 1911).

This method works in the same computational way that the Chinese used five centuries ago under the name of '*the celestial element method*'. This way substantially equivalent to Horner's method was described in detail by Qin Jiushao in the first half of the thirteenth

CONTACT F. Laudano ✉ flaud@katamail.com, flaudano@unisa.it

© 2019 Informa UK Limited, trading as Taylor & Francis Group

century, although it had its origins much earlier in the procedures for root extraction (Smoryski, 2007).

In Europe it was François Vite who around year 1600 made the first attempt to find a general solution to nonlinear polynomial equations by approximation (Montucla, 1800). The method consisted of an algorithm, with which the equations' root digits were obtained, one by one, together with tables that made it easier to continue with the process. This method became the foundation of the general way ('*via generalis*') of solving equations during great part of the seventeenth century and it made up the foundation of Horner and Newton's methods. The method was adopted and improved by mathematicians such as Thomas Harriot (1560–1621), William Oughtred (1574–1660), Pierre Hérigone (1580–1643), John Pell (1611–1685) or François Dechales (1621–1678) among others. Subsequently, Newton's method was introduced for the approximate resolution of numerical equations, in which method the root's approximate values, both commensurable and incommensurable, are obtained through an iterative process at a speed just surpassed by Horner (Ling & Needham, 1954).

After Newton, Simpson, Daniel Bernoulli and Euler dealt with the problem but none of them could make further progress. Lagrange propounded his own method (Lagrange, 1826) which was successful in theory avoiding Newton's defects, but it was much more complicated in practice. Horner made Lagrange's method easier by working out the root in decimal form digit by digit instead of expressing the root in the form of a continued fraction.

As is well-known, the Remainder Theorem and the Factor Theorem are more generally valid for polynomials with coefficients in a generic domain (cf. (Mac Lane Birkhoff, 1985, Corollaries 1 and 2, p. 162)), and recently it has been extended to polynomials over arbitrary coefficient rings (Dobbs, 2007, Theorem 2.1 and Corollary 2.2). These results are very useful for calculating the remainder and for testing the divisibility by polynomials of type $x{-}c$, because they avoid the long division method (cf. (Mac Lane Birkhoff, 1985, Theorem 21, p. 161)), with a significant reduction in calculations.

It is natural to ask whether the technique of substitution-evaluation can be applied to polynomials other than $x{-}c$. Let, for example,

$$f(x) = 2x^{15} + 5x^3 + x^2 - 3x + 3 \quad \text{and} \quad m(x) = x^3 - 2 \in \mathbb{Z}[x],$$

substituting 2 for x^3 in $f(x)$ we obtain

$$2 \cdot 2^5 + 5 \cdot 2 + x^2 - 3x + 3 = 64 + 10 + x^2 - 3x + 3 = x^2 - 3x + 77$$

which, as can be easily checked, is exactly the remainder of $f(x)$ on division by $m(x)$. Then $x^3 - 2$ does not divide $2x^{15} + 5x^3 + x^2 - 3x + 3$ in $\mathbb{Z}[x]$. Moreover, $f(\alpha) = \alpha^2 - 3\alpha + 77$ where α is a root of $m(x)$.

Note that the topics stated above can be also stated in terms of resultants (see Lang, 2002, Chapter IV, § 8 for their precise definition), both the bezoutian and the resultant matrix came in the eighteenth century from Eulers work in elimination theory (Wimmer, 1990). It is well known that the resultant of two polynomials $\operatorname{Res}(p(x), q(x))$ can be expresed in terms of the diferences of their roots and it is 0 if $p(x)$ and $q(x)$ have a common root. It is easy to check that $\operatorname{Res}(p(x), x - a) = p(a)$ if $p(x)$ is a monic polynomial, moreover, if both

$p(x)$ and $q(x)$ are monic

$$\mathrm{Res}(p(x), q(x)) = \prod_{\alpha \text{ root of } q(x)} p(\alpha).$$

Resultants can be computed in any unique factorization domain and they behave well under ring specialization. As mentioned before they are commonly defined as the determinant of a Sylvester matrix whose entries are related to the coefficients of the polynomials. When one wants to compute the resultant in an efficient way one has to take into accout the so called 'invariance under change of polynomials ' property that involves the Euclidean algorithm for polynomials. That is, the resultant of two successive remainders differs from the resultant of the initial polynomials by a controlable factor involving the leading coefficients and this leads again to our approach. Following the example above it is clear that

$$\mathrm{Res}(f(x), m(x)) = \mathrm{Res}(x^2 - 3x + 77, m(x)) = \prod_{\alpha \text{ root of } m(x)} \alpha^2 - 3\alpha + 77.$$

Thus indeed a deep understanding of the remainder-division algorithm is a key point in an abstract algebra course involving elimination (resultants) theory.

As a final remark, note that the technique used in the example can be rephased in a computer language as a rewriting rule $x^3 \rightarrow 2$ or more generally, if $m(x) = x^n - \sum_{i=0}^{n-1} a_i x^i$ the rule $x^n \rightarrow \sum_{i=0}^{n-1} a_i x^i$ used recursively. Note that again the understanding the remainder-division algorithm would lead a good introduction to the multivariable case and the obstacles and how to avoid them when you tackle more that one variable. In this sense note that gcd, the rewritting rule and remainders are just the univariate instances of Gröbner basis computation, reductions and elements under the *scalier* (Cox, Little, & O'Shea, 2015).

It is therefore appropriate to consider whether the substitution method may be extended to other polynomials $m(x)$ to enrich the learning proccess. This seems to be a very natural question that is not clearly highlighted in the literature. In the following pages we will show that this is possible. Theorem 2.5 provides concurrently a generalization of the classical Division Algorithm and of Remainder Theorem over arbitrary (possibly non-commutative) coefficient rings R. From this result an algorithm will follow that calculates the remainder of the division by any non-constant polynomial m whose leading coefficient is a unit in R (see Remark 2.4). From Theorem 2.5, we will also obtain Theorem 2.7, which provides an extension to the classical Factor Theorem and, hence, a general divisibility criterion for polynomials over arbitrary coefficient rings (see Remark 2.5).

2. General polynomial remainder theorem

In the following h, j, k, and n denote natural numbers; R denotes a *non-trivial* ring but need not be commutative; and $R[x]$ denotes the set of all polynomials with coefficients in R in an indeterminate x. Moreover it is assumed, for each $a \in R$, to satisfy $xa = ax$.

Let a and b be elements of R. If there exists an element x in R with $ax = b$, one says that a is a left divisor of b in R and that b is a right multiple of a. Similarly, if there exists an element y in R with $ya = b$, one says that a is a right divisor of b and that b is a left multiple of a. One says that a is a two-sided divisor of b if it is both a left divisor and a right divisor of b; in this case, it is not necessarily true that $x = y$, only that both some x and some y exist in R, each of which satisfies the appropriate equation.

As in the ring of integer, we can define the following relation in R, called '*left* modulo-m congruence'.

Definition 2.1: Let $m, a, b \in R$. We say that a is *left-m*-congruent to b in R, and we write $a \equiv_m^l b$ if and only if there exist $q \in R$ such that $a - b = qm$.

The following proposition can be proved simply by translating in R the techniques typically used for integers.

Proposition 2.2: *The left modulo-m congruence is an equivalence relation that preserves the addition of R.*

Remark 2.1: Note that in general the *left* modulo-m congruence relation does not preserves the product of R. In fact in the ring of 2×2 matrix over the real numbers, we have the following counterexample. Let

$$m := \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}, \quad a := \begin{pmatrix} 3 & 2 \\ 0 & -4 \end{pmatrix}, \quad b := \begin{pmatrix} 3 & 1 \\ 0 & -6 \end{pmatrix}, \quad c := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$d := \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$$

we have: $a \equiv_m^l b$, $c \equiv_m^l d$, but $ac \not\equiv_m^l bd$. In fact $ac - bd = \begin{pmatrix} 0 & 6 \\ 0 & -10 \end{pmatrix}$. The two products are not right congruent though.

To obtain our main result, we recall some other notion of basic algebra.

Definition 2.3: An element $u \in R$ is called a right-unit (left-unit) of R if there exists $v \in R$ with $vu = 1$ ($uv = 1$). The element v is called left-inverse of u (right inverse of u). If an element $u \in R$ is both a left and a right unit, we will say that u is a unit f R.

Remark 2.2: Let $a \in R$. If there exist $u, v \in R$ that are respectively the right and the left inverse of a, we have $u = 1u = (va)u = v(au) = v1 = v$. In this case there is a unique inverse of a and we can denotes it by a^{-1}.

Definition 2.4: If $m = a_h x^h + a_{h-1} x^{h-1} + \cdots + a_1 x + a_0 \in R[x]$ and $a_h \neq 0$, then a_h is called the leading coefficient of m, h is called its degree and is denoted by $deg(m)$.

Remark 2.3: Let $f, m, s \in R[x]$, and let $x^h \equiv_m^l s$ with $deg(f) \geq h$. Since $R[x]$ is a ring for any $g \in R[x]$ we have: $gx^h - gs = g(x^h - s) = gqm$ for some $q \in R[x]$, i.e. $gx^h \equiv_m^l gs$. In the following we will say that the polynomial gs was obtained right-substituting (or right-replacing) s for x^h in f. Thus Proposition 2.2 shows that the polynomial obtained by right-substituting s for x^h in f is *left* modulo-m congruent to f.

With the following theorem, using the *left*-modulo-m congruence relation, we extend over arbitrary (possibly non-commutative) rings the Euclidean Algorithm. This theorem is often stated over a coefficient field (cf. Rotman, 2003, Theorem 3.21, p. 131), or over arbitrary coefficient domains (cf. Mac Lane & Birkhoff, 1985, Theorem 21, p. 161; Rotman, 2003, Exercise 3.32, p. 142), or also over arbitrary coefficient commutative rings (cf. Lang, 2002, Theorem 1.1, p. 173). Recently a generalization has been found for polynomials on commutative rings (Laudano, 2018, Theorem 2.7). We can now prove the main theorem.

Theorem 2.5 (General Remainder Theorem – Euclidean Algorithm over arbitrary – possibly non-commutative-rings): *Let* R *be a ring, let* f *a polynomial of* $R[x]$ *of degree* $n > 1$ *and let* $m = a_h x^h + a_{h-1}x^{h-1} + \cdots + a_1 x + a_0 \in R[x]$ *whose leading coefficient* a_h *is a unit of* R*. Then*:

(1) *There exist unique polynomials* $q,\ r \in R[x]$ *such that* $f = qm + r$*, where* $r = 0$ *or* $deg(r) < deg(m)$*. Moreover If* $deg(f) \geq h$*, then* r *can be found by right-substituting the polynomial* $t = a_h^{-1}(-a_{h-1}x^{h-1} - \cdots - a_1 x - a_0)$ *for* x^h *in* f*, and iterating this substitution in the polynomial thus obtained until its degree becomes less than* h*.*

(2) *There exist unique polynomials* $p,\ s \in R[x]$ *such that* $f = mp + s$*, where* $s = 0$ *or* $deg(s) < deg(m)$*. Moreover If* $deg(f) \geq h$*, then* s *can be found by left-substituting the polynomial* $t = a_h^{-1}(-a_{h-1}x^{h-1} - \cdots - a_1 x - a_0)$ *for* x^h *in* f*, and iterating this substitution in the polynomial thus obtained until its degree becomes less than* h*.*

(3) *Let* q, r, p*, and* s *be as in* (1) *and* (2)*. Examples show that it need not be the case that* $q = p$*; and it need not be the case that* $r = s$*.*

Proof: (1) We have $f = 0m + f$; then if $f = 0$ or $deg(f) < h$ the existence of q and r is proved. Let us now analyse the case $n = deg(f) \geq h$. Since a_h is a unit of R, then there exists $a_h^{-1} \in R$, and, therefore, the polynomial $t \in R[x]$. In addition, $x^h \equiv^l_m t$ because $x^h - t = a_h^{-1}m$. Therefore, by Remark 2.3, the polynomial f_1 obtained by right-replacing x^h with t in f is *left-m*-congruent to f; thus, there exists $a \in R[x]$ such that $f = am + f_1$. Hence, if $deg(f_1) < h$ the existence is proved. Otherwise, we can observe that $deg(f_1) < deg(f)$ because x^h has been replaced with a polynomial t of degree less than h; then, repeating this replacement in f_1, we obtain a polynomial f_2 that is *left-m*-congruent to f_1 and having $deg(f_2) < deg(f_1)$. Iterating at most $k = n{-}h + 1$ times the previous replacement, we obtain a sequence of polynomials $f_1, f_2, \ldots, f_k \in R[x]$ with $f \equiv^l_m < f_1 \equiv^l_m \cdots \equiv^l_m </ f_k$ and $deg(f_k) \leq n - k = h - 1$. So the existence of q and r is proved.

As for uniqueness, suppose that $f = q_1 m + r_1 = q_2 m + r_2$, with $deg(r_1)$ and $deg(r_2) < deg(m)$, then we have $(q_1 - q_2)m = r_2 - r_1$ so $q_1 \neq q_2$ if and only if $r_1 \neq r_2$, in which case we have $deg((q_1 - q_2)m) = deg(q_1 - q_2) + deg(m) = deg(r_2 - r_1) < deg(m)$ and from this contradiction we conclude that $q_1 = q_2$ and $r_1 = r_2$.

(2) The proof follows the one developed in the previous item.

(3) An example of polynomials q, r, p, and s verifying the last condition can be found in Dobbs (2007, p. 270). For convenience we report it below. R is the ring $\mathbb{H}$ of quaternions over the real numbers (i.e. the ring of all expression of the form $a + bi + cj + dk$, where a, b, c, d are real numbers, and $-1 = i^2 = j^2 = k^2$, with the usual operations). Moreover is assumed that $xa = ax$ for each $a \in \mathbb{H}$, and $m{:} = x{-}j$.

'In the first example, we take $f := ix^2$; and in the second example, we take $f := x^2 + (i - j)x - k$. It only remains to exhibit the associated left and right quotients and remainders, as follows: $ix^2 = (ix+k)(x-j) + (-i) = (x-j)(ix-k) + (-i)$ and $x^2 + (i-j)x - k = (x+i)(x-j) + 0 = (x-j)(x+i) + (-2k)$’. ■

The polynomials q and r above are, respectively, called the *left*-quotient and the *left*-remainder of f on division by m, and, in the following, the polynomial r and q are also called ‘remainder and quotient of f *left*-modulo m’.

Remark 2.4: The procedure in the previous proof ends in a finite number of steps; therefore, it provides an algorithm. We will call this procedure the GR-algorithm. It calculates the *left*-remainder of f modulo m in $R[x]$ without running the long division method.

Let us now try to use the above result for polynomials over non-commutative coefficient rings.

Example 2.6: We want to calculate the *left*-remainder of

$$f = \begin{pmatrix} 4 & 0 \\ -1 & 2 \end{pmatrix} x^3 - x + \begin{pmatrix} 0 & 4 \\ 7 & -1 \end{pmatrix} \text{ left} - \text{modulo } m = x^2 - \begin{pmatrix} 1 & 3 \\ -2 & 0 \end{pmatrix}$$

in $M_2\mathbb{R}[x]$, the polynomial ring over the ring of 2×2 matrix on real numbers.

In this case, $s = \left(\begin{smallmatrix} 1 & 3 \\ -2 & 0 \end{smallmatrix}\right)$, i.e. $x^2 \equiv^l_m \left(\begin{smallmatrix} 1 & 3 \\ -2 & 0 \end{smallmatrix}\right)$, and right-substituting s for x^2 in f we have

$$\begin{aligned} f &= \begin{pmatrix} 4 & 0 \\ -1 & 2 \end{pmatrix} x^2 x - x + \begin{pmatrix} 0 & 4 \\ 7 & -1 \end{pmatrix} \equiv^l_m \begin{pmatrix} 4 & 0 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ -2 & 0 \end{pmatrix} x - x + \begin{pmatrix} 0 & 4 \\ 7 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 4 & 12 \\ -5 & -3 \end{pmatrix} x - x + \begin{pmatrix} 0 & 4 \\ 7 & -1 \end{pmatrix} = \begin{pmatrix} 3 & 12 \\ -5 & -4 \end{pmatrix} x + \begin{pmatrix} 0 & 4 \\ 7 & -1 \end{pmatrix} \end{aligned}$$

which has a degree less than $deg(m)$, and, therefore, is the remainder of f *left*-modulo m in $M_2\mathbb{R}[x]$.

It is clear that the above considerations can be used to test the *left*-divisibility between the polynomials of $R[x]$. In fact, as a corollary of the previous theorem, we obtain the following generalization of the classical Factor Theorem.

Theorem 2.7 (General Factor Theorem over arbitrary – possibly non-commutative-coefficient ring): *Let R be a ring, let f a polynomials of $R[x]$ of degree $n \geq h$ and let $m = a_h x^h + a_{h-1}x^{h-1} + \cdots + a_1 x + a_0 \in R[x]$ with $h > 0$ If a_h is a unit of R, the following statements are equivalent:*

(a) *m is a right divisor of f in $R[x]$*
(b) *right-substituting the polynomial $s = a_h^{-1}(-a_{h-1}x^{h-1} - \cdots - a_1 x - a_0)$ for x^h in f and iterating this substitution in the polynomial thus obtained at most $n-h+1$ times, we obtain the zero polynomial.*

Proof: m is a right divisor of f in $R[x]$ if and only if the left-remainder of f *left*-modulo m is 0. For Theorem 2.5, this remainder is provided by right-replacing x^h with the polynomial $t = a_h^{-1}(-a_{h-1}x^{h-1} - \cdots - a_1 x - a_0)$ in f and iterating this replacement in the polynomial thus obtained at most $n-h+1$ times. The result follows. ■

Remark 2.5: The General Factor theorem provides a finite procedure that is useful for testing the divisibility among polynomials over a coefficient ring, without running the long division method. We will call this procedure the GF-algorithm.

The following examples show how to use it.

Example 2.8: Let $\mathbb{H}$ be the ring of quaternions. We want to test whether the polynomial

$$m = x^3 - 2ix + 1 \text{ is a left divisor of } f = x^7 - 2ix^5 + x^4 + kx^3 + 2jx + k \text{ in } \mathbb{H}[x].$$

In this case $s = 2ix{-}1$ then, right-replacing x^3 with $2ix{-}1$ in f, we have

$$f \equiv_m (2ix - 1)^2 x - 2i(2ix - 1)x^2 + (2ix - 1)x + k(2ix - 1) + 2jx + k = \cdots = 4jx.$$

Then m is not a *left*-divisor of f in $\mathbb{H}[x]$.

Example 2.9: Let $\mathbb{Z}[i]$ be the ring of Gaussian integers (i.e. the ring of all complex numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$ and $i^2 = -1$, with the usual operations). We want to test whether the polynomial

$$m = ix^2 + 4 \text{ divides } f = x^7 - 2ix^5 + 8x^3 - (1 + i)x^2 + 4i - 4 \text{ in } \mathbb{Z}[i][x].$$

The leading coefficient of m is a unit in $\mathbb{Z}[i]$ and $s = i^{-1}(-4) = 4i$; thus, replacing x^2 with $s = 4i$ in f, we have $f \equiv_m\ x(4i)^3 - 2ix(4i)^2 + 8x(4i) - (1 + i)(4i) + 4i - 4 = 0$. Then m divides f in $\mathbb{Z}[i][x]$.

It is clear that the classical Remainder Theorem and the Factor Theorem are obtained by placing $m = x{-}c$ in Theorems 2.5 and 2.7. More generally, if $m = x^h - c$ and f are polynomials over R, with $deg(f) \geq h > 0$, then the remainder of f *left*-modulo m can be found by right-substituting c for x^h in f. Therefore, we obtain the following theorem.

Theorem 2.10 (Remainder Theorem for polynomials of type $x^h - c$): *Let R be a ring, and let $c \in R, f \in R[x]$, with $n = deg(f) \geq h > 0$. Let $n = kh + t$, where k and t are integers with $0 \leq t < h$, and let $a_{hk+u} = 0$ for any integer u with $h > u > t$. The remainder of f left-modulo $x^h - c$ is the polynomial obtained right-substituting c for x^h in f, and grouping the coefficients of terms having an equal degree.*

Proof: Since $a_{hk+u} = 0$ for any integer u with $h > u > t$, by placing $m = x^h$, we can write

$$f = a_{hk+(h-1)}x^{hk+(h-1)} + a_{hk+(h-2)}x^{hk+(h-2)} + \cdots + a_2x^2 + a_1x + a_0,$$

and from $(x^h)^j \equiv_m^l c^j$, we have $x^{hj+t} = x^{hj}x^t = (x^h)^j x^t \equiv_m^l c^j x^t$. The result follows. ■

Example 2.11: We want to calculate the remainder of

$$f = 2x^{13} - 3x^{11} + 4x^8 - 2x^4 + x + 1 \text{ modulo} m = x^5 + 2 \text{ in } \mathbb{Z}[x].$$

In this case, $n = 13$ and $h = 5$, and, therefore, the quotient on division of n by h is $k = 2$ and the remainder is $r = 3$; thus, we can write f as $2x^{5\cdot 2+3} - 3x^{5\cdot 2+1} + 4x^{5\cdot 1+3} - 2x^4 +$

$x+1$. Then, applying Theorem 2.10, being $a_{14}=a_{5\cdot 2+4}=0$, we have the remainder

$$\begin{aligned} r &= (a_4+a_9c+a_{14}c^2)x^4+(a_3+a_8c+a_{13}c^2)x^3+(a_2+a_7c+a_{12}c^2)x^2 \\ &\quad +(a_1+a_6c+a_{11}c^2)x+(a_0+a_5c+a_{10}c^2) \\ &= (-2+0+0)x^4+(0-8+8)x^3+(0+0+0)x^2+(1+0-12)x+(1+0+0) \\ &= -2x^4-11x+1. \end{aligned}$$

Then, m does not divide f in $\mathbb{Z}[x]$.

By the previous theorem, we can derive the following result.

Theorem 2.12 (Factor Theorem for polynomials of type x^h-c): *Let R be a ring, and let $c\in R, f\in R[x]$, with $n=deg(f)\geq h>0$. Let k and t be the quotient and the remainder on division of n by h, and let $a_{hk+u}=0$ for any integer u with $h>u>t$. The polynomial x^h-c is a left-divisor of f if and only if for any $l\in\{1,2,\dots,h\}$ we have*

$$\sum_{j=0}^{k}a_{hj+(h-l)}c^j=0.$$

Example 2.13: We want to test whether the polynomial

$$m=x^4+k \text{ is a left divisor of } f=x^7-2ix^5+x^4+kx^3+2jx+k \text{ in } \mathbb{H}[x].$$

In this case, calculating $\sum_{j=0}^{1}a_{4j+(4-l)}(-k)^j$ with $l\in\{1,2,\dots,h\}$, we have

$$\sum_{j=0}^{1}a_{4j+3}(-k)^j=(k+(-k))=0,\quad \sum_{j=0}^{1}a_{4j+2}(-k)^j=(0+0)=0,$$

$$\sum_{j=0}^{1}a_{4j+1}(-k)^j=(2j-2i(-k))=0,\quad \sum_{j=0}^{1}a_{4j+4}(-k)^j=(k+(-k))=0.$$

Then m is a *left*-divisor of f in $\mathbb{H}[x]$.

Definition 2.14: In abstract algebra, a division ring (cf. Lam & Leroy, 1988; Martínez-Penas, 2018), also called a skew field (cf. Smits, 1968), is a ring in which division is possible. Specifically, it is a non-zero ring in which every non-zero element a has a multiplicative inverse, i.e. an element x with $ax=xa=1$. Stated differently, a ring is a division ring if and only if the group of units equals the set of all non-zero elements. A division ring is a type of non-commutative ring.

Since every *non-zero* element of a division ring is a unit, we can also try the next Corollaries of Theorems 2.5 and 2.7.

Corollary 2.15 (General Remainder Theorem over a coefficient division ring): *Let F be a division ring; let $f,m\in F[x]$ with $m=a_hx^h+a_{h-1}x^{h-1}+\cdots+a_1x+a_0$ and $h>0$; and let $a_h\neq 0$.*

(a) *If $f = 0$ or $deg(f) < h$, then the left-remainder of f modulo m in $F[x]$ is f.*
(b) *If $deg(f) \geq h$, then the left-remainder of f modulo m in $F[x]$ can be found by right-substituting the polynomial $s = a_h^{-1}(-a_{h-1}x^{h-1} - \cdots - a_1x - a_0)$ for x^h in f and iterating this substitution in the polynomial thus obtained until its degree becomes less than h.*

Corollary 2.16 (General Factor Theorem over a coefficient division ring): *Let F be a division ring, and let $f, m \in F[x]$ with $m = a_hx^h + a_{h-1}x^{h-1} + \cdots + a_1x + a_0$, $grad(f) \geq h > 0$ and $a_h \neq 0$. The following statements are equivalent:*

(a) *m is a right divisor of f in $F[x]$*
(b) *right-substituting the polynomial $s = a_h^{-1}(-a_{h-1}x^{h-1} - \cdots - a_1x - a_0)$ for x^h in f and iterating this substitution in the polynomial thus obtained at most $n-h+1$ times, we obtain the zero polynomial.*

Example 2.17: We want to test whether the polynomial

$$m = 5x^2 + 3ix - j \text{ is a right divisor of } f = 25x^4 - 19x^2 + k \text{ in } \mathbb{H}[x].$$

The leading coefficient of m is $5 \neq 0$ and $s = 5^{-1}(-3ix + j)$. Then, right-replacing x^2 with s in f, we have:

$$f \equiv_m 25\left(\frac{-3ix+j}{5}\right)^2 - 19\frac{-3ix+j}{5} + k = -9x^2 + 0 - 1 + \frac{57ix - 19j}{5} + k \equiv_m \frac{27ix - 9j}{5} - 6kx - 1 + \frac{57ix - 19j + 5k}{5} = \cdots \neq 0.$$

Therefore, m is not a *left*-divisor of f in $\mathbb{H}[x]$.

3. An epilogue: skew polynomial rings

In this final section we will point to some known results for evaluating and dividing on skew polynomial rings. This will show the potential of the topic all around the mathematical instruction, note that also this approach has been used actually in applied mathematics as for example in coding theory (see for example Martínez-Penas, 2018). We will rectrict ourselves to skew polynomial rings over fields with no derivation but the same results can be stated easily for general skew polynomial rings over division rings (Lam & Leroy, 1988). Let F be a field and σ an automorphism of F. The skew polynomial ring $R = F[x, \sigma]$ is the set of polynomials over the field F where the addition is defined as the usual one in the polynomial ring $F[x]$ and the multiplication is defined as follows

$$\left(ax^i\right)\left(bx^j\right) = a\sigma^i(b)x^{i+j} \quad a, b \in F,\ i, j \in \mathbb{N}.$$

Indeed it a non-commutative ring unless σ is the identity. One can see that the Euclidean algorithm holds for right division which implies that R is a left principal ideal domain (Lam & Leroy, 1988). So following the previous sections we can evaluate a (left) polynomial

$f(x) = \sum_{i=0}^{k} a_i x^i$ on $a \in F$. Note that the obviuous 'evaluation' $\sum_{i=0}^{k} a_i x^i$ is wrong since it does not take into account the action of σ, but if we define

$$\mathcal{N}_{\sigma,i}(a) = \prod_{j=0}^{i-1} \sigma^j(a) \quad \text{for } i > 0, \text{ and } \mathcal{N}_{\sigma,0} = 1$$

whe have the following Factor Theorem

Theorem 3.1 (Jacobson, 1996, Proposition 1.3.11): *Let* $f(x) = \sum_{i=0}^{k} a_i x^i \in R$. *Then*

(a) *The remainder* r *on right division of* $f(x)$ *by* $x{-}a$ *is given by* $r = \sum_{i=0}^{k} a_i \mathcal{N}_{\sigma,i}(a)$.
(b) $(x - b)$ *divides (on the right)* $f(x)$ *if and only if* $\sum_{i=0}^{k} a_i \mathcal{N}_{\sigma,i}(b) = 0$.

Note that both a, b in the theorem above can be in a extension of F and, by abuse of notation, we will call σ also to the extension of the original automorphism. Also some ideas in the introduction can be extended to this type of rings; see, for example, a nice construction of the resultant of non-commutative polynomials in Erić (2008). Also the Euclidean division on the ring $F[x, \sigma]$ has been described in Caruso and Le Borgne (2012, Section 2.1.2). Thus it is easy to conclude a 'generalized evaluation-remainder theorem' in terms of the evaluation on the roots of the quotient polynomial as the evaluation of the remainder.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

A. Cuida http://orcid.org/0000-0002-9682-0825
F. Laudano http://orcid.org/0000-0003-4489-095X
E. Martinez-Moro http://orcid.org/0000-0003-1243-2049

References

Blitzer R. (2014). *Precalculus* (5th ed.). Miami: Pearson.
Caruso X., & Le Borgne J. (2012). *Some algorithms for skew polynomials over finite fields*. Preprint, arXiv:1212.3582.
Cajori F. (1911). Horner's method of approximation anticipated by Ruffini. *Bulletin of the American Mathematical Society*, 17(8), 409–414.
Cox D. A., Little J., & O'Shea D. (2015). *Ideals, varieties, and algorithms an introduction to computational algebraic geometry and commutative algebra* (4th ed.). Undergraduate Texts in Mathematics. Cham: Springer.
Dobbs D. E. (2007). The remainder theorem and factor theorem for polynomials over noncommutative coefficient rings. *International Journal of Mathematical Education in Science and Technology*, 38(2), 268–273. doi:10.1080/00207390600913350
Erić A. Lj. (2008). The resultant of non-commutative polynomials. *Matematicki Vesnik*, 60(1), 3–8.
Jacobson N. (1996). *Finite dimensional division algebras over fields*. New York, NY: Springer.
Joseph G. (2011). *The crest of the peacock: Non-European roots of mathematics*. Princeton, NJ: Princeton University Press.

Lagrange J. L. (1826). *Traité de la résolution des équations numériques de tous les degrés: avec des notes sur plusieurs points de la théorie des équations algébriques* (p. 126). Paris: Bachelier.

Lam T. Y., & Leroy A. (1988). Vandermonde and Wronskian Matrices over Division Rings. *Journal of Algebra*, 119, 308–336.

Lang S. (2002). *Algebra* (3rd ed.). New York, NY: Springer-Verlag.

Laudano F. (2018). A generalization of the remainder theorem and factor theorem. *IJMEST*. doi:10.1080/0020739X.2018.1522676

Ling W., & Needham J. (1954). Horner's method in Chinese mathematics: Its origins in the root-extraction procedures of the Han dynasty. *T'oung Pao -+ International Journal of Chinese Studies*, 43(1), 345–401. doi:10.1163/156853254X00146

Mac Lane S., & Birkhoff G. (1985). *Algebra*. Milano: Mursia.

Martínez-Penas U. (2018). Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring. *Journal of Algebra*, 504, 587–612. doi:10.1016/j.jalgebra.2018.02.005

McAskill B., Watt W., Balzarini E., Johnson B., Kennedy R., Melnyk T., & Zarski C. (2012). *Precalculus 12*. New York, NY: McGraw-Hill Ryerson.

Montucla J. (1800). *Histoire des mathématiques* (Vol. 2, 3:3, pp. 601–603). Paris.

Rotman J. J. (2003). *Advanced modern algebra*. New York, NY: Prentice-Hall.

Smits T. H. M.. (1968). Skew polynomial rings. *Nederlandse Akademie van Wetenschappen. Proceedings. Series A. Indagationes Mathematicae* (Vol. 71). doi:10.1016/S1385-7258(68)50022-2.

Smoryski C. (2007). *History of mathematics: A supplement*. New York: Springer Science & Business Media.

Wimmer H. K. (1990, January). On the history of the Bezoutian and the resultant matrix. *Linear Algebra and its Applications*, 128, 27–34.